4. Dispose of paper records following appropriate record destruction procedures. (See §310.13(c) and DoD 5200.1–R.)

E. TECHNICAL SAFEGUARDS

1. Components are to ensure that all PII not explicitly cleared for public release is protected according to Confidentially Level Sensitive, as established in DoD Instruction 8500.2. In addition, all DoD information and data owners shall conduct risk assessments of compilations of PII and identify those needing more stringent protection for remote access or mobile computing.

2. Encrypt unclassified personal information in accordance with current Information Assurance (IA) policies and procedures, as issued.

3. Remove personal data stored on magnetic storage media by methods that preclude reconstruction of the data.

4. Ensure that personal information is not inadvertently disclosed as residue when transferring magnetic media between activities.

5. Only DoD authorized devices shall be used for remote access. Any remote access, whether for user or privileged functions, must conform to IA controls specified in DoD Instruction 8500.2.

6. Remote access for processing PII should comply with the latest IA policies and procedures.

7. Minimize access to data fields necessary to accomplish an employee's task-normally, access shall be granted only to those data elements (fields) required for the employee to perform his or her job rather than granting access to the entire database.

8. Do not totally rely on proprietary software products to protect personnel data during processing or storage.

F. SPECIAL PROCEDURES

1. Managers shall:

a. Prepare and submit for publication all system notices and amendments and alterations thereto. (See §310.30(f).)

b. Identify required controls and individuals authorized access to PII and maintain updates to the access authorizations.

c. When required, ensure Privacy Impact Assessments are prepared consistent with the requirements of the DoD Deputy Chief Information Officer Memorandum, ''DoD Privacy Impact Assessment Guidance,'' October 28, 2005.

d. Train all personnel whose official duties require access to the system of records in the proper safeguarding and use of the information and ensure that they receive Privacy Act training.

G. RECORD DISPOSAL

1. Dispose of records subject to this Regulation so as to prevent compromise. (See §310.13(c).) Magnetic tapes or other magnetic medium may be cleared by degaussing, overwriting, or erasing. (See DoD Memorandum, ''Disposition of Unclassified DoD Computer Hard Drives,'' June 4, 2001.)

2. Do not use respliced waste computer products containing personal data.

APPENDIX B TO PART 310—SAMPLE NOTIFICATION LETTER

(See §310.14 of subpart C)

Dear Mr. John Miller:

On January 1, 2006, a Department of Defense (DoD) laptop computer was stolen from the parked car of a DoD employee in Washington, DC after normal duty hours while the employee was running a personal errand. The laptop contained personally identifying information on 100 DoD employees who were participating in the xxx Program. The compromised information is the name, social security number, residential address, date of birth, office and home email address, office and home telephone numbers of the Program participants.

The theft was immediately reported to local and DoD law enforcement authorities who are now conducting a joint inquiry into the loss.

We believe that the laptop was the target of the theft as opposed to any information that the laptop might contain. Because the information in the laptop was password protected and encrypted, we also believe that the probability is low that the information will be acquired and used for an unlawful purpose. However, we cannot say with certainty that this might not occur. We therefore believe that you should consider taking such actions as are possible to protect against the potential that someone might use the information to steal your identity.

You should be guided by the actions recommended by the Federal Trade Commission at its Web site at *http://www.consumer.gov/idtheft/con_steps.htm*. The FTC urges that you immediately place an initial fraud alert on your credit file. The Fraud alert is for a period of 90 days, during which, creditors are required to contact you before a new credit card is issued or an existing card changed. The site also provides other valuable information that can be taken now or in the future if problems should develop.

The DoD takes this loss very seriously and is reviewing its current policies and practices with a view of determining what must be changed to preclude a similar occurrence in the future. At a minimum, we will be providing additional training to personnel to ensure that they understand that personally identifiable information must at all times be treated in a manner that preserves and protects the confidentiality of the data.

We deeply regret and apologize for any inconvenience and concern this theft may cause you.

Should you have any questions, please call _____.

Sincerely,

Signature Block
(Directorate level or higher)

APPENDIX C TO PART 310—DOD BLANKET ROUTINE USES

(See paragraph (c) of §310.22 of subpart E)

A. ROUTINE USE—LAW ENFORCEMENT

If a system of records maintained by a DoD Component to carry out its functions indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or by regulation, rule, or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the agency concerned, whether Federal, State, local, or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, rule, regulation, or order issued pursuant thereto.

B. ROUTINE USE—DISCLOSURE WHEN REQUESTING INFORMATION

A record from a system of records maintained by a Component may be disclosed as a routine use to a Federal, State, or local agency maintaining civil, criminal, or other relevant enforcement information or other pertinent information, such as current licenses, if necessary to obtain information relevant to a Component decision concerning the hiring or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant, or other benefit.

C. ROUTINE USE—DISCLOSURE OF REQUESTED INFORMATION

A record from a system of records maintained by a Component may be disclosed to a Federal agency, in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decision on the matter.

D. ROUTINE USE—CONGRESSIONAL INQUIRIES

Disclosure from a system of records maintained by a Component may be made to a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of that individual.

E. ROUTINE USE—PRIVATE RELIEF LEGISLATION

Relevant information contained in all systems of records of the Department of Defense published on or before August 22, 1975, may be disclosed to the Office of Management and Budget in connection with the review of private relief legislation as set forth in OMB Circular A–19 at any stage of the legislative coordination and clearance process as set forth in that circular.

F. ROUTINE USE—DISCLOSURES REQUIRED BY INTERNATIONAL AGREEMENTS

A record from a system of records maintained by a Component may be disclosed to foreign law enforcement, security, investigatory, or administrative authorities to comply with requirements imposed by, or to claim rights conferred in, international agreements and arrangements, including those regulating the stationing and status in foreign countries of Department of Defense military and civilian personnel.

G. ROUTINE USE—DISCLOSURE TO STATE AND LOCAL TAXING AUTHORITIES

Any information normally contained in Internal Revenue Service (IRS) Form W–2 which is maintained in a record from a system of records maintained by a Component may be disclosed to State and local taxing authorities with which the Secretary of the Treasury has entered into agreements under 5 U.S.C., sections 5516, 5517, 5520, and only to those State and local taxing authorities for which an employee or military member is or was subject to tax regardless of whether tax is or was withheld. This routine use is in accordance with Treasury Fiscal Requirements Manual Bulletin No. 76–07.

H. ROUTINE USE—DISCLOSURE TO THE OFFICE OF PERSONNEL MANAGEMENT

A record from a system of records subject to the Privacy Act and maintained by a Component may be disclosed to the Office of Personnel Management (OPM) concerning information on pay and leave, benefits, retirement reductions, and any other information necessary for the OPM to carry out its legally authorized government-wide personnel management functions and studies.

I. ROUTINE USE—DISCLOSURE TO THE DEPARTMENT OF JUSTICE FOR LITIGATION

A record from a system of records maintained by a Component may be disclosed as a routine use to any component of the Department of Justice for the purpose of representing the Department of Defense, or any